AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims

1-12. (Canceled)

13. (Currently Amended) A virus trap computer system for protecting a host computer system from an intrusion such as a computer virus or an unauthorized access, said virus trap computer system comprising:

an embedded personal computer coupled to ~~said~~ the host computer system, said embedded personal computer ~~capable of~~ receiving all external computer communications that are directed to ~~said~~ the host computer system; ~~and capable of detecting said intrusion before said intrusion reaches said host computer system~~

means for monitoring the external computer communications and detecting whether the intrusion is present in the external computer communications; and

a password controller coupled to the embedded personal computer and a network interface, said password controller receiving an external communication from the network interface, identifying a password in the external communication, and in response to receiving a valid password, allowing the external communication access to the embedded personal computer.

14. (Currently Amended) The virus trap computer system as set forth in claim 13 wherein ~~said~~ the virus trap computer system is capable of deleting ~~said~~ the intrusion by erasing data within ~~said~~ the virus trap computer system.

15. (Currently Amended) The virus trap computer system as set forth in claim 14 wherein ~~said~~ the data erased by ~~said~~ the virus trap computer system comprises one of:

a computer virus software program, an operating system of ~~said~~ the virus trap computer system, and at least one computer software program within ~~said~~ the virus trap computer system.

16. (Currently Amended) The virus trap computer system as set forth in claim 14 wherein after ~~said~~ the virus trap computer system has deleted ~~said~~ the intrusion by erasing data within ~~said~~ the virus trap computer system, ~~said~~ the virus trap computer system is capable of receiving a clean version of data that existed in ~~said~~ the virus trap computer system before ~~said~~ the intrusion occurred.

17. (Currently Amended) The virus trap computer system as set forth in claim 16 ~~wherein said virus trap computer system comprises~~ further comprising a restoration controller for ~~capable of~~ supplying to ~~said~~ the virus trap computer system ~~said~~, the clean version of ~~said~~ the data after ~~said~~ the virus trap computer system has deleted ~~said~~ the intrusion by erasing data within ~~said~~ the virus trap computer system.

18. (Currently Amended) The virus trap computer system as set forth in claim 16 wherein ~~said~~ the virus trap computer system ~~is capable of receiving said~~ receives the clean version of ~~said~~ the data from one of: (1) ~~said~~ the host computer system, and (2) an external backup copy of ~~said~~ the clean version of ~~said~~ the data.

19. (Currently Amended) The virus trap computer system as set forth in claim 13 ~~wherein said virus trap computer system comprises~~ further comprising a peripheral switch that ~~is capable of switching~~ switches control of at least one computer peripheral from ~~said~~ the virus trap computer system to ~~said~~ the host computer system and from ~~said~~ the host computer system to ~~said~~ the virus trap computer system.

20. (Currently Amended) The virus trap computer system as set forth in claim 19 further comprising a ~~hardware~~ control switch coupled to ~~said~~ the host computer system, said ~~hardware~~ control switch capable of causing ~~said~~ the peripheral switch of ~~said~~ the virus trap computer system to switch control of said at least one computer peripheral from ~~said~~ the virus trap computer system to ~~said~~ the host computer system.

21. (Currently Amended) The virus trap computer system as set forth in claim 13 further comprising:

a data transfer switch coupled to ~~said~~ the embedded personal computer and ~~coupled~~ to ~~said~~ the host computer system;

wherein ~~said~~ the data transfer switch ~~is capable of transferring~~ transfers data from ~~said~~ the host computer system to ~~said~~ the embedded personal computer when ~~said~~ the data transfer switch is set in read only mode; and

wherein ~~said~~ the data transfer switch ~~is capable of transferring~~ transfers data from ~~said from said~~ the embedded personal computer to ~~said~~ the host computer system and from ~~said~~ the host computer system to ~~said~~ the embedded personal computer when ~~said~~ the data transfer switch is set in read and write mode.

22. (Currently Amended) The virus trap computer system as set forth in claim 21 wherein ~~said~~ the data transfer switch is exclusively controlled by ~~said~~ the host computer system.

23. (Currently Amended) The virus trap computer system as set forth in claim 13 further comprising:

a mass storage device coupled to ~~said~~ the embedded personal computer; and

a restoration controller coupled to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device, said restoration controller ~~capable of~~ for (1) causing all data on ~~said~~ the embedded personal computer and ~~said~~ the mass storage device to be erased, and (2) after ~~said~~ the data has been erased, supplying a clean version of ~~said~~ the erased data to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device.

24. (Currently Amended) The virus trap computer system as set forth in claim 23 further comprising:

a mass storage integrity controller coupled to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device, said mass storage integrity controller ~~capable of~~ for detecting an intrusion on ~~said~~ the mass storage device, and ~~capable of~~ requesting ~~said~~ the embedded personal computer to cause ~~said~~ the restoration controller to cause all data on ~~said~~ the mass storage device to be erased.

25. (Canceled)

26. (Currently Amended) The virus trap computer system as set forth in claim [[25]] 13 wherein ~~said~~ the password controller is coupled to ~~said~~ the host computer system, and wherein ~~said~~ the host computer system, in response to receiving a valid second level password from ~~said~~ the password controller, ~~is capable of allowing said computer~~ allows the external communication access to ~~said~~ the host computer system through ~~said~~ the embedded personal computer and through ~~said~~ a data transfer switch.

27. (Canceled)

28. (Currently Amended) ~~The virus trap computer system as set forth in claim 27 further comprising~~ A virus trap computer system for protecting a host computer system from an intrusion such as a computer virus or an unauthorized access, said virus trap computer system comprising:

an embedded personal computer coupled to the host computer system, said embedded personal computer receiving all external computer communications that are directed to the host computer system, and detecting an intrusion before the intrusion reaches the host computer system;

a mass storage device coupled to the embedded personal computer;

a mass storage integrity controller coupled to the embedded personal computer and to the mass storage device, said mass storage integrity controller detecting an intrusion on the mass storage device;

a restoration controller coupled to the embedded personal computer and to the mass storage device, said restoration controller deleting the intrusion by erasing data within the embedded personal computer and within the mass storage device, said restoration controller thereafter supplying a clean version of the erased data to the embedded personal computer and to the mass storage device; and

a password controller coupled to ~~said~~ the embedded personal computer and ~~coupled~~ to a network interface, said password controller ~~capable of (1)~~ receiving a computer communication from ~~said~~ the network interface, ~~and (2)~~ identifying a password in ~~said~~ the computer communication, and ~~(3)~~ in response to receiving a valid password, allowing ~~said~~ the external computer communication access to one of: ~~said~~ the embedded personal computer and ~~said~~ the host computer system.

29. (Currently Amended) The virus trap computer system as set forth in claim [[27]] 28 wherein ~~said~~ the embedded personal computer, ~~said~~ the restoration controller, and ~~said~~ the mass storage integrity controller are implemented on one integrated circuit chip.

30. (Currently Amended) The virus trap computer system as set forth in claim 28 wherein ~~said~~ the embedded personal computer, ~~said~~ the restoration controller, ~~said~~ the mass storage integrity controller, and ~~said~~ the password controller are implemented on one integrated circuit chip.

31-36. (Canceled)

37. (Currently Amended) A method ~~for~~ of protecting a host computer system from an intrusion such as a computer virus or an unauthorized access, said method comprising ~~the steps of~~:

coupling a virus trap computer system to ~~said~~ the host computer system, said virus trap computer system comprising an embedded personal computer coupled to ~~said~~ the host computer through a data transfer switch;

coupling a password controller to the embedded personal computer and to a network interface;

receiving ~~in said embedded personal computer all external computer communications that are~~ a computer communication in the password controller from the network interface, said computer communication being directed to ~~said~~ the host computer system; [[and]]

identifying a password in the computer communication;

in response to receiving a valid password, sending the external computer communication to the embedded personal computer for transfer to the host computer system; and

detecting ~~said~~ the intrusion ~~in said~~ by the embedded personal computer before ~~said~~ the intrusion reaches ~~said~~ the host computer system.

38. (Currently Amended) The method as set forth in claim 37 further comprising the step of:

deleting ~~said~~ the intrusion by erasing data within ~~said~~ the virus trap computer system.

39. (Currently Amended) The method as set forth in claim 38 wherein ~~said~~ the data erased by ~~said~~ the virus trap computer system comprises one of: a computer virus software program, an operating system of ~~said~~ the virus trap computer system, and at least one computer software program within ~~said~~ the virus trap computer system.

40. (Currently Amended) The method as set forth in claim 38 further comprising the step of:

after ~~said~~ the step of deleting the intrusion ~~has been deleted by erasing data within said virus trap computer system~~, receiving in ~~said~~ the virus trap computer system, a clean version of data that existed in ~~said~~ the virus trap computer system before ~~said~~ the intrusion occurred.

41. (Currently Amended) The method as set forth in claim 40 wherein ~~said~~ the clean version of the data is provided by one of: ~~(1)~~ a restoration controller in ~~said~~ the virus trap computer system, ~~and (2) said~~ the host computer system, and ~~(3)~~ an external backup copy of ~~said~~ the clean version of ~~said~~ the data.

42. (Currently Amended) The method as set forth in claim 37 further comprising the steps of:

switching control of at least one computer peripheral ~~from said~~ between the virus trap computer system ~~to said~~ and the host computer system according to host computer system requirements ~~and from said host computer system to said virus trap computer system with~~ utilizing a peripheral switch in ~~said~~ the virus trap computer system; and

using a ~~hardware~~ control switch coupled to ~~said~~ the host computer system to cause ~~said~~ the peripheral switch of ~~said~~ the virus trap computer to switch control of said at least one computer peripheral from ~~said~~ the virus trap computer system to ~~said~~ the host computer system.

43. (Currently Amended) The method as set forth in claim 37 further comprising the steps of:

coupling a data transfer switch to ~~said~~ the embedded personal computer and to ~~said~~ the host computer system;

transferring data from ~~said~~ the host computer system to ~~said~~ the embedded personal computer when ~~said~~ the data transfer switch is set in read only mode;

transferring data from ~~said~~ the embedded personal computer to ~~said~~ the host computer system and from ~~said~~ the host computer system to ~~said~~ the embedded personal computer when ~~said~~ the data transfer switch is in read and write mode; and

exclusively controlling ~~said~~ the data transfer switch with ~~said~~ the host computer system.

44. (Currently Amended) The method as set forth in claim 37 further comprising the steps of:

coupling a mass storage device to ~~said~~ the embedded personal computer;

coupling a restoration controller to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device;

in response to a signal from ~~said~~ the restoration controller, causing all data on ~~said~~ the embedded personal computer and on ~~said~~ the mass storage device to be erased; and

after ~~said~~ the data has been erased, ~~supplying~~ transferring a clean version of ~~said~~ the erased data to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device.

45. (Currently Amended) The method as set forth in claim 44 further comprising the steps of:

coupling a mass storage integrity controller to ~~said~~ the embedded personal computer and to ~~said~~ the mass storage device;

detecting an intrusion in ~~said~~ the mass storage device with ~~said~~ the mass storage integrity controller; and

requesting ~~said~~ the embedded personal computer to ~~cause said~~ instruct the restoration controller to erase ~~cause~~ all data on ~~said~~ the mass storage device ~~to be erased.~~

46. (Canceled)

47. (Currently Amended) The method as set forth in claim [[46]] 37 further comprising the steps of:

coupling ~~said~~ the password controller to ~~said~~ the host computer system; and

in response to receiving a valid second level password in ~~said~~ the password controller, allowing ~~said~~ the external computer communication access to ~~said~~ the host computer system through ~~said~~ the embedded personal computer and through ~~said~~ the data transfer switch.

48. (New) A virus trap for protecting an associated host computer from a computer virus received from an external source, said virus trap comprising:

a mass storage device that stores data and application programs;

an embedded processor that controls the virus trap and runs the application programs;

means for receiving communications from the external source and supplying the communications to the embedded processor;

an integrity controller that monitors the data and application programs to detect unauthorized read or write operations;

a restoration controller, responsive to a detection of an unauthorized read or write operation, for taking corrective action to erase corrupted data and/or applications associated with the detected unauthorized read or write operation, and to restore the erased data and/or applications with uncorrupted data and/or applications;

a data transfer switch that transfers data to or from the host computer; and

a password controller that verifies a password received from the external source and allows access to the data transfer switch only when the password controller positively verifies the password.

49. (New) A virus trap for protecting an associated host computer from a computer virus received from an external source, said virus trap comprising:

a mass storage device for storing data and application programs;

an embedded processor for controlling the virus trap and running the application programs;

a password controller for receiving and verifying a first-level password from the external source;

means, responsive to a positive verification of the first-level password, for receiving communications from the external source and supplying the communications to the embedded processor;

an integrity controller for monitoring the data and application programs to detect unauthorized read or write operations; and

a restoration controller, responsive to a detection of an unauthorized read or write operation, for taking corrective action to erase corrupted data and/or applications associated with the detected unauthorized read or write operation, and to restore the erased data and/or applications with uncorrupted data and/or applications.

50. (New) The virus trap of claim 49, further comprising a data transfer switch connected to the host computer, wherein access to the data transfer switch is granted only when the password controller positively verifies a second-level password received from the external source.

51. (New) The virus trap of claim 50, wherein the password controller notifies the host computer that the second-level password has been positively verified, and the host computer activates the data transfer switch in response.

52. (New) The virus trap of claim 51, wherein the host computer activates the data transfer switch in a unidirectional mode allowing only data transfers from the host computer to the virus trap.

53. (New) The virus trap of claim 51, wherein the host computer activates the data transfer switch in a bi-directional mode allowing data transfers from the host computer to the virus trap and from the virus trap to the host computer.

54. (New) The virus trap of claim 53, wherein the host computer deactivates the data transfer switch if no data is transferred for a predefined time period.

55. (New) The virus trap of claim 49, wherein the integrity controller also monitors an operating system for the embedded processor.

56. (New) The virus trap of claim 55, wherein the restoration controller includes a memory for storing uncorrupted operating system software for the embedded processor.

57. (New) The virus trap of claim 56, wherein the memory in the restoration controller also stores uncorrupted data and/or application programs.

58. (New) The virus trap of claim 49, wherein the integrity controller sends a non-maskable interrupt to the embedded processor when an unauthorized read or write operation is detected, said interrupt causing the embedded processor to send an alert to a user of the host computer.

59. (New) The virus trap of claim 58, wherein the restoration controller takes the corrective action when instructed to do so by the user of the host computer.

60. (New) The virus trap of claim 58, wherein the restoration controller takes the corrective action automatically upon determining either (1) corruption to the data or applications programs is severe, or (2) the user of the host computer does not respond to the alert for a predefined time period.

61 (New) The virus trap of claim 49, wherein the restoration controller performs a high-level restoration in which only data address tables are erased and restored, upon determining that the corruption to the data or application programs is not severe.

62. (New) The virus trap of claim 49, wherein the restoration controller performs a low-level restoration in which all data, application programs, and the operating system of the embedded processor are erased and restored, upon determining that the corruption to the data or application programs is severe.